Openbaar Ministerie

College van Procureurs-Generaal

Voorzitter

Postbus 20305 2500 EH Den Haag

Prins Clauslaan 16
2595 AJ Den Haag
Telefoon +31 (0)70 339 96 00
telefax +31 (0)70 339 98 51

De Minister van Veiligheid en Justitie
mr. I.W. Opstelten
Postbus 20301
2500 EH DEN HAAG

0BD

Onderdeel	Afdeling Wet- en Regelgeving	Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen
Contactpersoon		
Doorkiesnummer(s)		
E-mail		
Datum	08 juli 2013	
Ons kenmerk		
Uw kenmerk		
Onderwerp	Advies conceptwetsvoorstel Computercriminaliteit III	

Geachte heer Opstelten,

Bij brief van 02 mei 2013 heeft u het College van procureurs-generaal gevraagd te adviseren over het conceptwetsvoorstel computercriminaliteit III met de bijbehorende memorie van toelichting. Het conceptwetsvoorstel bevat voorstellen tot wijziging van het Wetboek van Strafvordering en het Wetboek van Strafrecht en beoogt de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken. Naast een aantal technische wijzigingen zijn in het wetsvoorstel vier onderwerpen opgenomen:

1. Voorgesteld wordt om een nieuwe bevoegdheid te creëren voor bepaalde opsporingsambtenaren, om in een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen ten behoeve van de opsporing van ernstige strafbare feiten;
2. De regeling van de bevoegdheid van de officier van justitie om, met machtiging van de rechter-commissaris, te bevelen dat gegevens op internet ontoegankelijk worden gemaakt, wordt verbeterd;
3. Er komt een afzonderlijke wettelijke bevoegdheid tot het geven van een bevel aan de verdachte tot het toegankelijk maken van versleutelde elektronische gegevens (decryptiebevel);
4. Heling van gegevens wordt strafbaar gesteld.

Met grote instemming heeft het College kennis genomen van het voornemen om heling van gegevens strafbaar te stellen en van het voorstel om een bevoegdheid te creëren voor opsporingsambtenaren om heimelijk op afstand een geautomatiseerd

werk binnen te kunnen dringen ten behoeve van de opsporing van ernstige strafbare feiten. Het College heeft derhalve met bijzondere belangstelling het wetsvoorstel gelezen en is gaarne bereid daarover te adviseren. De verschillende onderwerpen zullen in dit advies worden besproken in de volgorde die in het wetsvoorstel wordt aangehouden, waarbij de meer technische opmerkingen in een apart artikelsgewijs onderdeel zullen worden opgenomen.

Onderzoek in een geautomatiseerd werk
Als eerste wil het College nog eens onderstrepen dat het voor de opsporing en vervolging van ernstige misdrijven van het grootste belang is dat dit onderdeel van het wetsvoorstel wordt ingevoerd. De ontwikkelingen op het terrein van technologie, internet en communicatie gaan razendsnel. De groei van het internet biedt een ongekende hoeveelheid kansen voor burgers en bedrijven door toenemende mogelijkheden voor communicatie en bedrijvigheid. Denk aan het toenemende gebruik van het internet voor het bankverkeer, aankopen doen bij webshops of simpel gesprekken voeren. Deze (economische) groei is ondenkbaar zonder het bestaan van vertrouwelijke communicatie. Over het algemeen heeft de groei van de informatiemaatschappij veel positieve ontwikkelingen tot gevolg gehad voor het dagelijkse leven van burgers. Maar tegelijkertijd moet worden vastgesteld dat ook in het criminele circuit in toenemende mate van nieuwe technologieën gebruik wordt gemaakt. Ook criminelen maken gebruik van encryptie om bestanden te beveiligen, gebruiken beveiligde communicatiediensten zoals Whatsapp, Skype en Viber en gebruiken anonieme hotspots en cloudcomputingdiensten.[1]
In de memorie van toelichting wordt in de drie betreffende paragrafen de huidige stand van zaken over deze nieuwe technieken en de problemen die de opsporing daarbij ondervindt zeer goed beschreven. Waar het om gaat is dat moderne vormen van communicatie en dataopslag worden gekenmerkt door een diffuse locatie van de gegevens en als de gegevens kunnen worden gelokaliseerd, dan zijn zij niet toegankelijk. Dit is een ontwikkeling die nog verder zal toenemen. Denk behalve aan de treffende voorbeelden die in de memorie van toelichting zijn opgenomen ook aan nieuwe activiteiten van de kabelmaatschappijen waar het gaat om het inrichten van hotspots. Over niet al te lange tijd zal door middel van het gemeenschappelijk gebruik van alle kabelmodems van de abonnees een groot deel van de Randstad fungeren als één grote hotspot. Het is onwerkbaar om de communicatie van de crimineel te onderscheppen die ergens op straat inlogt op deze gemeenschappelijke hotspot. Men weet immers niet van welk kabelmodem hij op welk moment gebruik maakt.

In de toekomst zal het praktisch gesproken alleen nog mogelijk zijn om communicatie

---

[1] Zie in dit verband ook paragraaf 9 van het recent verschenen rapport van Europol over de Italiaanse maffia: Threat assesment, Italian organised crime, juni 2013

te onderscheppen op het moment dat deze wordt ingevoerd in de computer, telefoon of tablet, dan wel op het moment dat de boodschap wordt ontvangen. Dit is het moment waarop de boodschap in het apparaat wordt gesproken, met toetsen wordt ingevoerd, het bestand met gegevens wordt beveiligd, dan wel, na decryptie, het bestand door de ontvanger wordt gelezen of beluisterd.

Vastgesteld moet worden dat de bevoegdheden van politie en het openbaar ministerie onvoldoende zijn toegesneden op deze nieuwe ontwikkelingen. Het is goed om te realiseren dat de bestaande strafvorderlijke bevoegdheden vooral zijn ingericht op communicatie die is te onderscheppen en kan worden begrepen, op databestanden die daadwerkelijk kunnen worden gevonden en gelezen, op gegevens en informatie die kan worden verkregen ook buiten de wil van de verdachte. Voor de huidige ongrijpbare communicatie en niet te kraken gegevens bieden zij onvoldoende soelaas. Het College is daarom verheugd dat in het Wetboek van Strafvordering een nieuwe bevoegdheid wordt opgenomen die de politie in staat stelt om op afstand heimelijk binnen te dringen in een geautomatiseerd werk dat bij een verdachte in gebruik is. Op deze wijze kan de aanwezigheid van gegevens worden vastgesteld voordat zij worden versleuteld, kunnen gegevens worden overgenomen voordat zijn ergens in de cloud worden opgeslagen, kan mogelijk een sleutel voor het decrypten van bestanden worden gevonden en kan communicatie worden opgenomen voordat deze wordt versleuteld. Wil de opsporing in staat worden gesteld om gelijke tred te houden met de moderne ontwikkelingen op het gebied van computers en internet, dan is deze bevoegdheid onmisbaar.

Recent is in de media een discussie gevoerd over het hacken van computers die zich in het buitenland zouden bevinden. Het College merkt in dit verband op dat er maar heel weinig situaties voorstelbaar zijn waarbij technisch weliswaar kan worden vastgesteld dat een bepaalde computer niet in Nederland staat, maar waarbij niet kan worden vastgesteld waar deze computer zich dan wel bevindt. Als een IP-adres als uitgangspunt wordt genomen, dan kan de plaats waar de computer zich bevindt worden gelokaliseerd. Daaruit blijkt waar ter wereld de computer zich bevindt en of in overleg met andere overheden moet worden getreden over vervolgstappen of dat een rechtshulpverzoek moet worden ingediend. Als de locatie van een systeem niet kan worden vastgesteld, dan kan ook niet worden vastgesteld dat de computer in het buitenland staat. In deze situatie geldt de ubiquiteitsleer, die met zich meebrengt dat meerdere plaatsen als locus delicti kunnen worden aangemerkt en Nederland rechtsmacht heeft. Zie hiervoor bijvoorbeeld een uitspraak van de rechtbank Breda, NJFS 2011, 34. Vanuit oogpunt van opsporing en vervolging bezien, is de discussie over hacken op computers in het buitenland vooral een academische discussie, die onvoldoende aansluit bij de bestaande praktijk.

De ontoegankelijkmaking van gegevens
Het Wetboek van Strafrecht voorziet in de mogelijkheid tot het ontoegankelijk maken van gegevens door een tussenpersoon die een telecommunicatiedienst verleent bestaande uit de doorgifte of opslag van gegevens die van een ander afkomstig zijn (artikel 54a Sr). Voorgesteld wordt de bevoegdheid om de vordering tot het ontoegankelijk maken van gegevens als afzonderlijke en zelfstandige bevoegdheid op te nemen in het Wetboek van Strafvordering. In de memorie van toelichting wordt er terecht op gewezen dat het huidige artikel 54a Sr in de praktijk tot problemen leidt, omdat in dit artikel zowel een strafuitsluitingsgrond als een bevelsbevoegdheid is opgenomen.
In het conceptwetsvoorstel dat in 2010 aan het College ter advisering is voorgelegd, was een vergelijkbaar voorstel opgenomen. Bij die gelegenheid heeft het College geadviseerd om geen aparte bevelsbevoegdheid in het Wetboek van Strafvordering op te nemen en artikel 54a Sr als een pure strafuitsluitingsgrond te formuleren. Dit advies was grotendeels ingegeven door het feit dat in deze tijd de gedragscode "Notice and Take Down" tot stand was gekomen en door een groot aantal internetproviders werd ondertekend. In de praktijk functioneerde deze gedragscode goed en er was dus geen reden voor een bevelsbevoegdheid van de officier van justitie.
Inmiddels is in deze situatie een kentering gekomen. In vergelijking met de situatie van 2010 zijn er veel internetproviders bij gekomen die de gedragscode niet ondersteunen. In de praktijk wordt het openbaar ministerie daarom in toenemende mate geconfronteerd met internetproviders die niet wensen mee te werken aan het ontoegankelijk maken van strafbare gegevens. Het College is derhalve van oordeel dat het nu voorliggende voorstel in deze tijd en onder deze omstandigheden in een behoefte voorziet.

Ingevolge het voorgestelde artikel 125p kan de officier van justitie een bevel tot ontoegankelijkmaking van gegevens richten tot de aanbieder van een communicatiedienst in geval van verdenking van ieder strafbaar feit. Het College meent dat met de keuze voor 'een strafbaar feit' het risico ontstaat dat het openbaar ministerie in de rol van internetpolitie wordt gedrongen. Het inzetten van deze bevoegdheid in gevallen waarin vaak de vrijheid van meningsuiting een rol speelt kan in de samenleving, terecht of niet, al snel de indruk wekken dat er sprake is van een openbaar ministerie in de rol van censurerende internetpolitie. Het College zou een dergelijke beeldvorming beslist willen vermijden en adviseert derhalve om de uitoefening van de bevoegdheid tot het geven van het bevel te beperken tot een verdenking van een strafbaar feit als bedoeld in artikel 67 Sv. Het criterium 'strafbaar feit als bedoeld in artikel 67 Sv' past ook beter bij het voorstel om het bevel slechts te geven na het verlenen van een machtiging door de rechter-commissaris en biedt de praktijk voldoende soelaas.

Decryptiebevel

Voorgesteld wordt om een afzonderlijke wettelijke bevoegdheid te creëren tot het geven van een bevel aan een verdachte tot het toegankelijk maken van versleutelde elektronische gegevens. Een dergelijk decryptiebevel kan alleen worden gegeven aan een verdachte van een terroristisch misdrijf of iemand die wordt verdacht van het vervaardigen, verspreiden en het bezit van kinderpornografie.

Het College begrijpt de reden waarom het voorstel wordt gedaan. Zoals in de memorie van toelichting terecht wordt opgemerkt, kan het voor een adequate bestrijding van zeer ernstige vormen van criminaliteit, waarmee de geestelijke gezondheid en de lichamelijke integriteit van slachtoffers ernstig kunnen worden aangetast en waarbij gebruik wordt gemaakt van elektronische gegevens, van groot belang zijn dat politie en justitie toegang kunnen krijgen tot versleutelde gegevens. Het College meent echter dat de invoering van een decryptiebevel op de wijze waarop het nu is vormgegeven op een aantal praktische en juridische bezwaren stuit.

Het is de vraag of het voorgestelde decryptiebevel en de daaraan gekoppelde strafbaarstelling verenigbaar is met het nemo-teneturbeginsel. Het College heeft kennis genomen van het rapport "Het decryptiebevel en het nemo-teneturbeginsel" van professor Koops.[2] De vraag of een decryptiebevel aan de verdachte kan worden gegeven, waaraan een strafbaarstelling wordt gekoppeld in geval van weigering, hangt van een viertal factoren af:

1. de aard en mate van dwang;
2. het gewicht van het maatschappelijk belang;
3. de aanwezigheid van relevante waarborgen in de procedure;
4. de manier waarop het afgedwongen materiaal wordt gebruikt.

Deze factoren worden als volgt gewogen: naarmate de dwang om mee te werken voor de verdachte groter is en het afgedwongen materiaal een zwaardere rol heeft bij het bewijs waarop de verdachte eventueel wordt veroordeeld, zal het maatschappelijk belang, de noodzaak om het bevel te geven, des te groter moeten zijn en zullen er meer waarborgen moeten zijn voor rechtsbescherming.
Uit de nemo-teneturjurisprudentie van het Europese Hof kan voorts worden afgeleid, nog steeds volgens het rapport, dat een eventueel van de verdachte afgedwongen decryptie van zijn bestanden alleen aanvaardbaar is als dit bevel zich beperkt tot bepaalde delicten waarbij versleuteling aantoonbaar een groot probleem veroorzaakt. Voorts dient de wetgever terughoudend te zijn met een instrumentele inzet van het strafrecht; de bedoeling is om misdadigers te straffen voor feiten die zij hebben begaan, niet om verdachten te straffen voor het niet meewerken aan bewijsgaring.

---

[2] Bert-Jaap Koops: Het decryptiebevel en het nemo-teneturbeginsel, september 2012, Universiteit van Tilburg.

Welnu, ziet het College het goed, dan is de conclusie dat een decryptiebevel onder een strafbedreiging wel aan de verdachte kan worden gegeven, maar alleen in zeer zwaarwegende omstandigheden, als laatste redmiddel, op het moment dat de overheid als het ware met de rug tegen de muur staat en niet anders meer kan.
Maar als dat zo is, dan is het aan te bevelen om het geven van een decryptiebevel niet te koppelen aan twee weliswaar ernstige, maar toch willekeurige type delicten zoals terroristische misdrijven en kinderpornografie (beroep of gewoonte). Er zijn binnen deze twee typen delicten tal van variaties mogelijk, waarbij het van de omstandigheden af zal hangen of zonder strijdigheid met het nemo-teneturbeginsel een decryptiebevel aan de verdachte kan worden gegeven. Voor wat betreft de terroristische misdrijven moet men zich realiseren dat daaronder ook een aantal minder ernstige delicten vallen, zoals brandstichting, waarbij het label "terroristisch misdrijf" wordt bepaald door het oogmerk waarmee de verdachte het misdrijf heeft begaan. Ook het delict kinderpornografie komt in allerlei gradaties voor, waaronder gevallen waarbij wel wordt vervolgd, maar waarvoor een lichte straf op zijn plaats is. Dit is ook mogelijk in het geval er wordt vervolgd voor het tweede lid van artikel 240b Sr, de beroeps- of gewoontevariant. In geval van recidive wordt al snel 'gewoonte' aangenomen, maar het kan zijn dat oude bestanden zijn aangetroffen, waarbij de slachtoffers of niet bestaan (virtuele kinderpornografie) of al lang uit het circuit van kinderpornografie zijn gehaald.
In relatie tot andere delicten zorgt de koppeling aan twee specifieke delicten voor een scheve verhouding binnen de strafvordering. Waarom kan de pleger van een brandstichting met terroristisch oogmerk wel een decryptiebevel worden gegeven en kan de vermoedelijke pleger van een moord niet worden verplicht de sleutel van het bestand te overhandigen waarin mogelijk informatie over de plaats van het verborgen lijk is te vinden? Waarom wordt het wel mogelijk de kinderpornograaf (240b Sr) een decryptiebevel te geven, maar degene die het kind heeft misbruikt (244 Sr) niet?

Het College is van oordeel dat het beter is om het onder strafdreiging geven van een decryptiebevel aan de verdachte niet te koppelen aan twee delicten, maar aan bepaalde specifieke omstandigheden. Het College stelt voor om het voorgestelde vierde lid van artikel 125k zodanig te wijzigen, dat een decryptiebevel slechts kan worden gegeven in geval van verdenking van een misdrijf waarop 8 jaar of meer gevangenisstraf staat en er aanwijzingen bestaan voor een concreet gevaar voor het leven of de vrijheid van een persoon of de veiligheid van de staat.

Op deze wijze kan het decryptiebevel worden gegeven in de situaties die er echt toe doen. Denk bijvoorbeeld aan een ontvoering, waarbij voor het leven van de ontvoerde moet worden gevreesd. Indien een verdachte kan worden aangewezen, wiens computer mogelijk informatie bevat over de verblijfplaats van de ontvoerde, maar de

informatie is versleuteld, dan is er een gerechtvaardigd belang om een decryptiebevel te geven. Mogelijk kan de ontvoerde daardoor worden gered.
Als het gaat om kinderpornografie, dan is een decryptiebevel op zijn plaats indien bestanden worden aangetroffen waarvan kan worden vermoed dat de slachtoffers nog in het 'circuit' van kinderpornografen zitten. Politie en justitie zullen alles op alles zetten om deze slachtoffers te redden. Dan is de urgentie aanwezig om een decryptiebevel te geven.
Deze voorbeelden kunnen met andere worden aangevuld. Waar het om gaat is dat de constructie zoals door het College wordt voorgesteld, beter past in het frame van uitzonderingen waarbij een gerechtvaardigde inbreuk kan worden gemaakt op het nemo-teneturbeginsel. Het gaat in dit voorstel om de urgentie, de noodzaak, waaronder het bevel wordt gegeven en het gaat niet meer in de eerste plaats om het rond krijgen van het strafrechtelijk bewijs, maar om het voorkomen van slachtoffers. Dat is de factor van het maatschappelijk belang dat zodanig zwaar weegt dat een inbreuk op het nemo-teneturbeginsel, gepaard gaande met forse dwangmiddelen zoals een strafdreiging, te verdedigen is.

Vervolgens is het de vraag of een decryptiebevel effectief kan zijn. Met een nieuw artikel 184b Sr wordt de weigering van de verdachte om gegevens te ontsleutelen strafbaar gesteld met een gevangenisstraf van ten hoogste drie jaar. De verdachte die opzettelijk niet voldoet aan het bevel tot het ontsleutelen van gegevens pleegt een misdrijf. Het opzet heeft betrekking op alle bestanddelen van het delict.
Het laatste maakt dat in de praktijk met de strafbepaling moeilijk zal kunnen worden gewerkt. Gevreesd moet worden dat in verreweg de meeste gevallen het bewijs van het opzet niet zal zijn te leveren. Bewijsnood zal in elk geval ontstaan in gevallen waarin de verdachte stelt dat hij zich de sleutel niet kan herinneren, bijvoorbeeld door de stress van zijn aanhouding, of dat hij de sleutel is verloren waardoor hij niet aan het bevel van de officier van justitie kan voldoen.
Wanneer vervolgens de voorgestelde strafmaat wordt bezien tegen de achtergrond van de straf die op de delicten zijn gesteld waarbij een decryptiebevel mogelijk is (vanaf maximaal 8 jaar gevangenisstraf), valt niet uit te sluiten dat de verdachte een eenvoudige rekensom maakt en ervoor kiest een veroordeling voor artikel 184b Sr te riskeren in plaats van een veroordeling voor het zwaardere delict. Om dit te vermijden zou de strafmaat van het niet opvolgen van het decryptiebevel welhaast gelijk moeten worden gesteld aan die van het gronddelict. Dat is geen oplossing die het College voor ogen staat. Wel geeft dit aan dat er een wezenlijk verschil bestaat tussen de strafdreiging voor het niet voldoen aan een decryptiebevel en de in de memorie van toelichting opgenomen voorbeelden die zijn gehaald uit de Wegenverkeerswet. Het niet meewerken aan een alcoholtest wordt net zo zwaar bestraft als het rijden onder invloed met een hoog promillage. Van het decryptiebevel mag in termen van effectiviteit dus niet al teveel worden verwacht.

Heling van digitale gegevens

Met dit onderdeel van het wetsvoorstel, opgenomen in de artikelen 138c en 138f, wordt voorzien in een al lang bestaande behoefte uit de praktijk. Met deze artikelen wordt de rechthebbende een betere strafrechtelijke bescherming geboden tegen personen die gegevens overnemen, aan anderen beschikbaar stellen en openbaar maken zonder dat er sprake is geweest van computervredebreuk. In het advies over het eerdere wetsvoorstel heeft het College gevraagd om een nadere toelichting op de wederrechtelijkheid. Deze uitleg wordt in paragraaf 5.3 gegeven. Inmiddels heeft ook de rechter zich uitgesproken over de wederrechtelijkheid van het overnemen van gegevens. De rechtbank Oost-Brabant heeft in LJN BZ1157 een handzaam kader geschetst aan de hand waarvan de wederrechtelijkheid kan worden getoetst. Bij de beoordeling of er sprake is van bijzondere omstandigheden die het wederrechtelijk karakter aan het handelen van verdachte doen ontvallen, zijn mede gelet op artikel 10 EVRM, drie factoren van belang. Ten eerste moet worden beoordeeld of verdachte heeft gehandeld in het kader van een wezenlijk maatschappelijk belang. Bij bevestigende beantwoording van deze vraag moet vervolgens worden bezien of het handelen van verdachte proportioneel was (ging verdachte niet verder dan noodzakelijk was om zijn doel te bereiken) en of er geen andere, minder vergaande manier was om het door de verdachte beoogde doel te kunnen bereiken (subsidiariteit). Het College adviseert om dit kader te betrekken bij de uitleg over de wederrechtelijkheid.

Overige opmerkingen

Het wetsvoorstel komt op een aantal punten tegemoet aan al lang bestaande wensen uit de praktijk. Er zijn echter nog een paar problemen waarvoor dit wetsvoorstel geen oplossing biedt. Het College adviseert om te overwegen voor de volgende problemen alsnog in een oplossing te voorzien.

Het succes van vele vormen van cybercrime is rechtstreeks afhankelijk van het bezit (gebruik) van een domeinnaam. Een domeinnaam die veel lijkt op die op die van een bank kan bezoekers aantrekken die een typefout maakten in een poging om de website van de bank te kunnen bezoeken (bijvoorbeeld wwx.ign.nl in plaats van wwx.ing.nl). Criminelen kunnen via dat gelijkende domein een website publiceren die sterk lijkt op die van de echte bank en via die website inlog gegevens voor internetbankieren bemachtigen. Een domeinnaam is steeds gekoppeld aan een IP-adres, maar hoewel het IP-adres kan wijzigen, is de domeinnaam een statisch gegeven.
Zowel de huidige als de voorgestelde voorzieningen voor ontoegankelijkmaking zien enkel op het ontoegankelijk maken van 'gegevens' en bieden geen mogelijkheid om organisaties die verantwoordelijk zijn voor de registratie van domeinnamen te bewegen om tot doorhaling van een registratie over te gaan of om een registratie over

te schrijven naar de overheid. Ook anderszins bestaan thans geen mogelijkheden om strafrechtelijk te interveniëren tegen het crimineel gebruik van domeinnamen. Een interventie tegen criminele infrastructuren op basis van IP-adressen is vele malen krachtiger wanneer tevens de domeinnaam wordt 'geneutraliseerd'. Het College adviseert daarom ook een wettelijke bevoegdheid te creëren waardoor het mogelijk wordt te bevelen dat een domeinnaam wordt doorgehaald of wordt overgeschreven naar de overheid.

Het tweede onderwerp betreft aanpassing van artikel 126bb, lid 5, Sv, in die zin dat de verplichting tot geheimhouding zich tevens uitstrekt tot het onderzoek dat ex artikel 125i Sv wordt uitgevoerd. In de opsporingspraktijk is het regelmatig noodzakelijk om gegevens veilig te stellen uit een geautomatiseerd werk bij een hostingprovider, zowel voor eigen opsporingsonderzoek of mogelijk ter uitvoering van een rechtshulpverzoek. Deze hostingproviders zijn weliswaar aan te merken als 'aanbieders' in de zin van artikel 125la Sv, maar zij vallen niet onder de Telecommunicatiewet. Op grond van de Telecommunicatiewet zijn aanbieders van openbare telecommunicatiediensten of netwerken, zoals ISP's of aanbieders van mobiele telefoondiensten, verplicht om opsporingshandelingen die ten aanzien van hun gebruikers plaatsvinden geheim te houden..
Dedicated hosting wordt niet aangemerkt als een openbare telecommunicatiedienst en artikel 125i Sv wordt niet genoemd in artikel 126bb, lid 5, Sv als een van de onderzoekshandelingen ter zake waarvan geheimhouding in acht dient te worden genomen. Dat maakt dat er een voortdurend afbreukrisico bestaat omdat verdachten voortijdig bekend raken met tegen hen verrichte opsporingshandelingen. Uit de praktijk blijkt dat een aantal (grote) webhostingsbedrijven hun klanten actief informeren omtrent een uitgevoerd onderzoek ex artikel 125i Sv. Het College adviseert derhalve om artikel 125i Sv op te nemen in het zesde lid van artikel 126bb Sv.

Hoogachtend
Het College van procureurs-generaal

Artikelsgewijs

Het wetboek van Strafrecht

Artikel 80sexies
De definitie van "geautomatiseerd werk" wordt gewijzigd. Onder een geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens te verwerken en op te slaan of over te dragen.
De vraag is of de voorgestelde definitie wel voldoet. Het onderscheid tussen het *opslaan, verwerken en overdragen* van gegevens lijkt gelet op de huidige stand van de techniek moeilijk vol te houden. In de recente 4Chan-zaak oordeelde de Hoge Raad bovendien (LJN BY9718) dat het begrip geautomatiseerd werk niet is beperkt tot apparaten die zelfstandig aan deze drievoudige eis kunnen voldoen, maar dat ook netwerken bestaande uit computers en/of telecommunicatievoorzieningen onder het begrip geautomatiseerd werk vallen. Het College adviseert om de definitie van geautomatiseerd werk aan te laten sluiten bij de internationaal erkende terminologie, in het bijzonder die van de Cybercrimeconventie van de Raad van Europa. In dit Cybercrimeverdrag wordt in artikel 1 onder een geautomatiseerd werk verstaan een inrichting, of een groep van verbonden inrichtingen, waarmee automatisch gegevens worden verwerkt.

Artikel 139e
In dit artikel wordt strafbaar gesteld degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijk plaats, een afbeelding vervaardigt. Deze uitvoerige omschrijving is onvoldoende specifiek en roept bijvoorbeeld de vraag op of foto's die op een feestje zijn gemaakt met een mobiele telefoon en waarvoor geen expliciete toestemming is gegeven, onder de delictsomschrijving valt. Het College meent dat het woord "heimelijk" meer recht doet aan de bedoeling van de strafbaarstelling dan het "niet op duidelijke wijze kenbaar maken" van het technisch hulpmiddel. De tekst van het artikel zou dan als volgt kunnen luiden:
"Met gevangenisstraf van ten hoogste zes maanden of een geldboete van de vierde categorie wordt gestraft degene die heimelijk, gebruik makende van een technisch hulpmiddel, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of een andere niet voor het publiek toegankelijke plaats, een afbeelding maakt."

Artikel 273d
Voor wat betreft artikel 273d Sr merkt het College op dat het tweede lid kan worden geschrapt indien in het eerste lid wordt aangesloten bij de definitie van artikel 126la Sv en de woorden "openbaar telecommunicatienetwerk of openbare

telecommunicatiedienst" worden vervangen door "communicatienetwerk of communicatiedienst".

Wetboek van Strafvordering

Artikel 67, lid 1, onderdeel b
Gelet op de omstandigheden waaronder het College meent dat een decryptiebevel moet kunnen worden gegeven, verdient het aanbeveling om ook artikel 184b in artikel 67, lid 1, onderdeel b op te nemen.

Artikel 125ja
Voor wat betreft de formulering van het voorgestelde artikel 125ja merkt het College het volgende op. In het eerste lid wordt het heimelijk binnentreden van een computer geregeld met het oog op verschillende doeleinden. In de onderdelen a t/m c mag worden binnengetreden met het oog op specifiek benoemde gevolgen. Zo mag worden vastgesteld of er bepaalde gegevens aanwezig zijn, kan de locatie worden bepaald, mogen bepaalde gegevens worden overgenomen of kan ervoor worden gezorgd dat bepaalde gegevens ontoegankelijk worden gemaakt.
In de onderdelen d t/m e wordt het heimelijk binnentreden van een computer in verband gebracht met de uitoefening van andere bijzondere opsporingsbevoegdheden. In dit geval is het duidelijk dat het bevel facilitair moet worden gezien aan de uitoefening van de genoemde opsporingsbevoegdheden. De vraag rijst daardoor, of de onderdelen a t/m c ook moeten worden gezien als facilitair aan andere opsporingsbevoegdheden en onderzoekshandelingen. Het ligt voor de hand om te veronderstellen dat de bevoegdheid tot het verrichten van de in de onderdelen a t/m c genoemde onderzoekshandelingen reeds ligt besloten in het bevel van artikel 125ja, maar geheel duidelijk is dat niet. Het wetsvoorstel dient op dit punt te worden verhelderd.

Het op afstand heimelijk binnendringen van een geautomatiseerd werk kan alleen indien de rechter-commissaris de officier van justitie machtigt tot het geven van het bevel. Tevens is in de memorie van toelichting in een procedure bij de CTC voorzien. Het College vreest een toename van administratieve lasten wanneer de toepassing van een van de in de onderdelen d t/m e genoemde opsporingsbevoegdheden eerst na het heimelijk binnentreden op grond van artikel 125ja mogelijk is. Met andere woorden, als eerst moet worden afgewacht of de resultaten van het heimelijk binnentreden een verdere inzet van bijzondere opsporingsbevoegdheden rechtvaardigen, dan levert dit extra administratie op en wordt ernstig afbreuk gedaan aan slagvaardig optreden. De verwachting is dat een praktijk zal ontstaan waarbij gelijktijdig met het bevel tot het binnentreden van een geautomatiseerd werk een bevel tot het uitoefenen van de overige opsporingsbevoegdheden zal worden gegeven. Op deze wijze kan worden

voorkomen dat de rechter-commissaris meerdere keren om een machtiging moet worden gevraagd en kan worden voorkomen dat de CTC meerdere keren moet worden gevraagd toestemming te geven. In dit verband adviseert het College om of in de artikelen genoemd in de onderdelen d t/m e een aparte verwijzing op te nemen naar artikel 125ja, zodat de uit te oefenen bevoegdheden in één bevel en in één machtiging kunnen worden opgenomen, of de onderdelen d t/m e zodanig te formuleren dat daaruit blijkt dat gelijktijdig met de daar genoemde bevoegdheden, het bevel van artikel 125ja kan worden gegeven en ook met één bevel en één machtiging kan worden volstaan.

Met een dergelijke verwijzing in de bestaande bevoegdheden kan tevens worden voorkomen dat er een opeenstapeling van technische certificering en verantwoording plaatsvindt. Zowel het voorgestelde artikel 125ja als een aantal van de onderdelen d t/m e genoemde opsporingsbevoegdheden bevatten voorschriften met betrekking tot de inzet van technische hulpmiddelen. In tenminste een aantal gevallen kan worden vastgesteld dat aan die middelen te stellen eisen overlappen en gevreesd moet worden dat dit leidt tot een verzwaring van de administratieve verantwoording waar het gaat om de gecombineerde inzet van bevoegdheden.

Ten slotte merkt het College op dat omdat in artikel 125ja de inzet van een technisch hulpmiddel wordt genoemd, dan tevens artikel 126ee Sv dient te worden gewijzigd in die zin, dat artikel 125ja erin moet worden opgenomen.

Artikel 125k
In de marge van het decryptiebevel wil het College wijzen op een daarmee verwant onderwerp. Op grond van de huidige wet mag de officier van justitie de ontsleuteling van een derde vorderen als het gaat om versleutelde gegevens die tijdens een doorzoeking ter vastlegging van gegevens zijn vastgelegd (artikel 125k, lid 1 Sv) of die eerder zijn gevorderd (artikel 126nh Sv) of getapt (artikel 126m, lid 6, Sv). Het is echter op dit moment niet mogelijk om de decryptie te vorderen van versleutelde bestanden in voorwerpen die in beslag zijn genomen op grond van de traditionele beslagartikelen (96 e.v. Sv). Er kan alleen 'onderzoek' worden gedaan aan het inbeslaggenomen voorwerp. In de praktijk worden echter met enige regelmaat versleutelde bestanden aangetroffen waarvan bekend is dat een derde die zou kunnen ontsleutelen. Het College adviseert om te overwegen ook voor dit probleem een voorziening te treffen.

Artikel 125p
De laatste volzin van het eerste lid van artikel 125p schrijft voor dat de verdachte is bevoegd zich bij het horen door een raadsman te doen bijstaan. Het College merkt op, mede gelet op de memorie van toelichting, dat hier waarschijnlijk is bedoeld degene tot wie het bevel is gericht. Deze is in dit stadium nog geen verdachte, het artikel dient

daarom te worden aangepast.
Een praktisch punt is nog wie wordt gehoord in het geval de aanbieder een rechtspersoon is. Wellicht kan de memorie van toelichting daarover nadere uitleg geven.

Het bevel kan worden gegeven aan een aanbieder van een communicatiedienst. Het College vraagt zich af waarom niet tevens een bevel kan worden gericht tot de aanbieder van een communicatienetwerk. Indien ook de aanbieder van een communicatienetwerk wordt geacht daarmee onder het begrip van een communicatiedienst te vallen, verdient het aanbeveling om dit in de memorie van toelichting nader uiteen te zetten.

In lid 2, onderdeel b, wordt voorgeschreven dat het bevel het strafbare feit dient te vermelden en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte. Het College vraagt zich af waarom de naam of aanduiding van de verdachte op het bevel dient te worden vermeld. De communicatieaanbieder hoeft alleen maar te weten dat de aard van bepaalde gegevens een strafbaar feit opleveren. Waarom moet hij ook weten wie de verdachte is? En als er geen verdachte bekend is en er ook geen nadere aanduiding kan worden gegeven van de verdachte, kan het bevel dan niet worden gegeven? Het College adviseert om dit deel van onderdeel a te schrappen.